ABSTRACT OF THE DISCLOSURE

A system for determining the validity of a received cryptographic message while ensuring for out-of-order messages is utilized to provide for secure communications among peers in a network. In particular, a secure communication module may be configured to accept the cryptographic message in response to a received nonce value of the received message is greater than the largest nonce value yet seen. Otherwise, when the received nonce value is not the largest nonce value yet seen, the secure communication module may be configured to compare the received nonce value with a nonce acceptance window. If the received nonce value falls outside the nonce acceptance window, the secure communication module may be further configured to reject the received message and assume that a replay attack has been detected. If the received nonce value falls within the nonce acceptance window, the secure communication module may be further configured to determine if the received nonce value has been seen before by comparing the received nonce value with a replay window mask. If the received nonce has been seen before, the secure communication module may be further configured to reject the received message and assume a replay attack. Otherwise, the secure communication module may be further configured to accept the message and add the received nonce value to the replay window mask.